

(Translation)

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : April 6, 2000

Application Number : Patent Appln. No. 2000-105525

Applicant(s) : MATSUSHITA ELECTRIC INDUSTRIAL  
CO., LTD.

Wafer  
of the  
Patent  
Office

January 19, 2001

Kozo OIKAWA  
  
Commissioner,  
Patent Office

Seal of  
Commissioner  
of  
the Patent  
Office

Appln. Cert. No.

Appln. Cert. Pat. 2000-3112877

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

J1002 U.S. PTO

09/828559



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 4月 6日

出 願 番 号

Application Number:

特願2000-105525

出 願 人

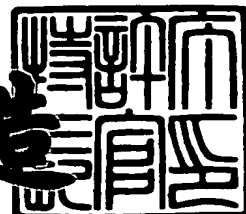
Applicant (s):

松下電器産業株式会社

2001年 1月19日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3112877

【書類名】 特許願

【整理番号】 2022510411

【提出日】 平成12年 4月 6日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 柴田 修

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 関部 勉

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100078282

【弁理士】

【氏名又は名称】 山本 秀策

【手数料の表示】

【予納台帳番号】 001878

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9303919

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 著作物保護システム、暗号化装置および復号化装置

【特許請求の範囲】

【請求項 1】 コンテンツ鍵を用いて暗号通信を行う暗号化装置および復号化装置から構成される著作物保護システムであって、

前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、

第 1 解読制限を更新して得られる第 2 解読制限に基づいて前記コンテンツ鍵を生成する第 1 コンテンツ鍵生成手段と、

前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第 1 暗号化手段とを具備し、

前記復号化装置は、前記第 2 解読制限から前記コンテンツ鍵を生成する第 2 コンテンツ鍵生成手段と、

前記暗号化コンテンツを前記第 2 コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第 1 復号化手段とを具備することを特徴とする著作物保護システム。

【請求項 2】 前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて前記第 2 解読制限に更新する解読制限更新手段と、

前記第 2 解読制限を時変鍵に基づいて暗号化し、第 1 暗号化解読制限を出力する第 2 暗号化手段とを具備し、

前記暗号化装置は、前記第 2 暗号化手段から転送される前記第 1 暗号化解読制限を前記時変鍵に基づいて復号化し、前記第 2 解読制限を生成する第 2 復号化手段とを具備し、

前記第 1 コンテンツ鍵生成手段は、前記第 2 復号化手段により生成された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成する、請求項 1 記載の著作物保護システム。

【請求項 3】 前記暗号化装置は、共通鍵を記憶する第 1 共通鍵記憶手段と

前記第 1 解読制限を記憶する解読制限記憶手段と、

第 1 乱数を生成する第 1 乱数発生手段と、

前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化装置と相互認証処理を行なう第 1 相互認証処理手段と、

前記第 1 相互認証処理手段における認証受理をうけて前記第 1 乱数と前記第 2 乱数とから前記時変鍵を生成する第 1 時変鍵生成手段と、

前記第 1 解読制限を前記時変鍵を用いて暗号化して第 2 暗号化解読制限を出力する第 3 暗号化手段とをさらに具備し、

前記復号化装置は、前記共通鍵を記憶する第 2 共通鍵記憶手段と、

前記第 2 乱数を生成する第 2 乱数発生手段と、

前記第 2 乱数と前記第 1 乱数とを用いて前記暗号化装置と相互認証を行なう第 2 相互認証処理手段と、

前記第 2 相互認証処理手段における認証受理をうけて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する第 2 時変鍵生成手段と、

前記第 2 暗号化解読制限を前記時変鍵を用いて復号化する第 3 復号化手段とを備える、請求項 2 記載の著作物保護システム。

【請求項 4】 前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて第 2 解読制限に更新する第 1 解読制限更新手段をさらに備え、

前記第 2 コンテンツ鍵生成手段は、前記第 1 解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成し、

前記暗号化装置は、前記復号化装置の第 1 解読制限更新手段における解読制限の更新をうけて、前記第 1 解読制限を解読制限更新則に従って前記第 2 解読制限に更新する第 2 解読制限更新手段をさらに備え、

前記第 1 コンテンツ鍵生成手段は、前記第 2 解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成する、請求項 1 記載の著作物保護システム。

【請求項 5】 前記暗号化装置は、前記共通鍵を記憶する第 1 共通鍵記憶手段と、

前記第 1 解読制限を記憶する解読制限記憶手段と、

第 1 乱数を生成する第 1 乱数発生手段と、

前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化

装置と相互認証を行なう第 1 相互認証処理手段と、

前記第 1 相互認証処理手段における認証受理をうけて前記第 1 乱数と前記第 2 乱数とから時変鍵を生成する第 1 時変鍵生成手段と、

前記第 1 解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第 2 暗号化手段とを具備し、

前記復号化装置は、前記共通鍵を記憶する第 2 共通鍵記憶手段と、

前記第 2 乱数を生成する第 2 乱数発生手段と、

前記第 2 乱数と前記第 1 乱数とを用いて前記暗号化装置と相互認証を行なう第 2 相互認証処理手段と、

前記第 2 相互認証処理手段における認証受理をうけて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する第 2 時変鍵生成手段と、

前記暗号化解読制限を前記時変鍵を用いて復号化する第 2 復号化手段とを具備する、請求項 4 記載の著作物保護システム。

【請求項 6】 前記第 2 解読制限更新手段は、予め前記第 1 解読制限を第 2 解読制限に更新し、

前記第 2 解読制限更新手段は、前記第 1 コンテンツ鍵生成手段に更新された前記第 2 解読制限を出力し、

前記第 1 コンテンツ鍵生成手段は、前記第 2 解読制限から前記コンテンツ鍵を生成し、

前記第 2 解読制限更新手段は、前記第 1 暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第 2 解読制限を格納する、請求項 5 記載の著作物保護システム。

【請求項 7】 前記第 1 および第 2 時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項 3 記載の著作物保護システム。

【請求項 8】 前記第 1 および第 2 コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項 3 記載の著作物保護システム。

【請求項 9】 前記暗号化装置および前記復号化装置は、前記暗号化装置お

よび前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、

前記第 1 および第 2 時変鍵生成手段は、前記第 1 および第 2 乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項 3 記載の著作物保護システム。

【請求項 1 0】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、

前記第 1 および第 2 時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項 3 記載の著作物保護システム。

【請求項 1 1】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、

前記第 1 および第 2 コンテンツ鍵生成手段は、前記第 2 解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成する、請求項 3 記載の著作物保護システム。

【請求項 1 2】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、

前記第 1 および第 2 コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項 3 記載の著作物保護システム。

【請求項 1 3】 前記第 1 および第 2 相互認証処理手段は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証する、請求項 3 記載の著作物保護システム。

【請求項 1 4】 コンテンツ鍵を用いて復号化装置と暗号通信を行う暗号化装置であって、

前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、

第 1 解読制限を更新して得られる第 2 解読制限に基づいて前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第 1 暗号化手段とを具備することを特徴とする暗号化装置。

【請求項 1 5】 前記暗号化装置は、前記復号化装置から転送される第 1 暗号化解読制限を時変鍵に基づいて復号化し、前記第 2 解読制限を生成する復号化手段を具備し、

前記コンテンツ鍵生成手段は、前記復号化手段により生成された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成する、請求項 1 4 記載の暗号化装置。

【請求項 1 6】 前記暗号化装置は、共通鍵を記憶する共通鍵記憶手段と、前記第 1 解読制限を記憶する解読制限記憶手段と、

第 1 乱数を生成する第 1 乱数発生手段と、

前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化装置と相互認証処理を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第 1 乱数と前記第 2 乱数とから前記時変鍵を生成する時変鍵生成手段と、

前記第 1 解読制限を前記時変鍵を用いて暗号化して第 2 暗号化解読制限を出力する第 2 暗号化手段とをさらに具備する、請求項 1 5 記載の暗号化装置。

【請求項 1 7】 前記暗号化装置は、前記復号化装置の解読制限の更新をうけて、前記第 1 解読制限を解読制限更新則に従って前記第 2 解読制限に更新する解読制限更新手段をさらに備え、

前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成する、請求項 1 4 記載の暗号化装置。

【請求項 1 8】 前記暗号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、

前記第 1 解読制限を記憶する解読制限記憶手段と、

第 1 乱数を生成する第 1 乱数発生手段と、

前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化



装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第 1 乱数と前記第 2 乱数とから時変鍵を生成する時変鍵生成手段と、

前記第 1 解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第 2 暗号化手段とを具備する、請求項 1 7 記載の暗号化装置。

【請求項 1 9】 前記解読制限更新手段は、予め前記第 1 解読制限を第 2 解読制限に更新し、

前記解読制限更新手段は、前記コンテンツ鍵生成手段に更新された前記第 2 解読制限を出力し、

前記コンテンツ鍵生成手段は、前記第 2 解読制限から前記コンテンツ鍵を生成し、

前記解読制限更新手段は、前記第 1 暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第 2 解読制限を格納する、請求項 1 8 記載の暗号化装置。

【請求項 2 0】 前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項 1 6 記載の暗号化装置。

【請求項 2 1】 前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項 1 6 記載の暗号化装置。

【請求項 2 2】 前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項 1 6 記載の暗号化装置。

【請求項 2 3】 前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項 1 6 記載の暗号化装置。

【請求項 2 4】 前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記データ系列鍵に基づい

て前記コンテンツ生成鍵を生成する、請求項 1 6 記載の暗号化装置。

【請求項 2 5】 前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項 1 6 記載の暗号化装置。

【請求項 2 6】 コンテンツ鍵を用いて暗号化装置と暗号通信を行う復号化装置であって、

前記復号化装置は、第 2 解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第 1 復号化手段とを具備することを特徴とする復号化装置。

【請求項 2 7】 前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて前記第 2 解読制限に更新する解読制限更新手段と、

前記第 2 解読制限を時変鍵に基づいて暗号化し、第 1 暗号化解読制限を出力する暗号化手段とを具備する、請求項 2 6 記載の復号化装置。

【請求項 2 8】 前記復号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、

前記第 2 乱数を生成する乱数発生手段と、

前記第 2 乱数と第 1 乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する時変鍵生成手段と、

第 1 暗号化解読制限を前記時変鍵を用いて復号化する第 2 復号化手段とを備える、請求項 2 7 記載の復号化装置。

【請求項 2 9】 前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて第 2 解読制限に更新する解読制限更新手段をさらに備え、

前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第

2 解読制限に基づいて前記コンテンツ鍵を生成する、請求項 2 6 記載の復号化装置。

【請求項 3 0】 前記復号化装置は、前記共通鍵を記憶する第 2 共通鍵記憶手段と、

前記第 2 乱数を生成する第 2 乱数発生手段と、

前記第 2 乱数と第 1 乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する時変鍵生成手段と、

暗号化解読制限を前記時変鍵を用いて復号化する第 2 復号化手段とを具備する、請求項 2 9 記載の復号化装置。

【請求項 3 1】 前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項 2 8 記載の復号化装置。

【請求項 3 2】 前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項 2 8 記載の復号化装置。

【請求項 3 3】 前記前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項 2 8 記載の復号化装置。

【請求項 3 4】 前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項 2 8 記載の復号化装置。

【請求項 3 5】 前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成する、請求項 2 8 記載の復号化装置。

【請求項 3 6】 前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項 2 8 記載の復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、解読制限を持った音楽、画像、映像、ゲームなどのデジタルコンテンツを機器間で共通鍵を共有化して暗号通信を行う通信システムにおいて、解読制限の更新が不正に行われた場合に解読できないようにしたものであり、共通鍵に解読制限の更新情報を関連させることによって著作物を保護するシステムに関する。

【0002】

【従来の技術】

近年、デジタル情報圧縮技術の進展とインターネットに代表されるグローバルな通信インフラの爆発的な普及によって音楽、画像、映像、ゲームなどのコンテンツをデジタル情報として通信回線を利用して各家庭に配信することが実現されはじめた。

【0003】

通信回線を利用したデジタル情報の配信サービスは、媒体によらないデータだけの流通形態であるため、配信サービス形態の自由度が飛躍的に向上し、単にコンテンツ情報を配信するだけでなく、使用回数、使用期間などの使用制限付きで配信させるなど、多様な形態で流通させることが可能である。

【0004】

デジタルコンテンツの著作権者の権利や流通業者の利益を保護した流通配信システムを確立するために、通信の傍受、盗聴、なりすましなどによる不正入手や、受信したデータを記憶した記録媒体における違法複製、違法改ざんなどの不正行為を防止することが課題となり、正規システムの判別、データスクランブルを行なう暗号／認証などの著作物保護技術が必要となる。

【0005】

著作物保護技術については従来より種々なものが知られており、代表的なものとしてデータの暗号化装置と復号化装置間で乱数、応答値の交換を行ない相互に正当性を認証し合い、正当である場合のみデータを送信するチャレンジレスポンス型の相互認証技術がある。

【0006】

本明細書において「解読制限」とは、暗号化装置から復号化装置に転送されたコンテンツを使用（再生して音をだすとか）してよいかの情報を意味する。例えば、再生回数付きのコンテンツの場合、解読制限は回数情報である。

【0007】

「解読制限の更新」とは、解読制限の更新則を意味する。例えば、再生回数付きのコンテンツの場合、暗号化装置から復号化装置に転送される解読制限（N回使用可能）の回数情報を1つ減らすことを意味する。

【0008】

「解読制限の更新情報」とは、更新された解読制限を意味する。例えば、再生回数付きのコンテンツの場合、暗号化装置から復号化装置に転送される解読制限（N回使用可能）が、解読制限の更新によって、解読制限の回数情報が「N-1回使用可能」と書き換えられた情報をさす。

【0009】

特に解読制限を持ったデジタルコンテンツを、前述の相互認証技術を用いて暗号通信を行なうシステムを考えた場合、データの暗号化装置と復号化装置間で相互に正当性を認証し合い、正当であると確認された時のみ解読制限を暗号化装置から復号化装置に暗号通信で転送し、復号化装置は解読制限を解釈して解読可能であるかを判定するとともに解読制限の更新情報を暗号化装置に暗号通信で送信したのち、コンテンツデータを暗号化装置から暗号通信でロードし解読して使用するのが一般的に行なわれる方法である。

【0010】

【発明が解決しようとする課題】

ここで課題となるのは、解読制限を記憶している解読制限の更新が正常に行なわれることであり、解読制限の更新が正常に行なわれていない場合、コンテンツ

を解読できないシステムが必要となる。

【 0 0 1 1 】

前述の相互認証技術では、通信する機器が正規なものかを判定するだけであり、必ずしも解読制限の更新が正常に行なわれたかを判定し、不正行為を防止するものではなく、解読制限の更新情報の転送のみを別の機器になりすまされた場合、問題となる。例えば、前述のシステムにおいて解読制限の更新情報の転送のみを別の機器になりすまされて処理された場合を考えると、解読制限の更新情報を復号化装置で暗号化して転送しても、転送先が正規の暗号化装置ではなく別の暗号化装置になりすまして処理した場合、正規の暗号化装置では解読制限の更新がなされないことになる。

【 0 0 1 2 】

本発明の目的は、解読制限の更新を確実に行なうとともに、デジタルコンテンツの不正解読を防止するシステムを提供することにある。

【 0 0 1 3 】

【課題を解決するための手段】

本発明に係る著作物保護システムは、コンテンツ鍵を用いて暗号通信を行う暗号化装置および復号化装置から構成される著作物保護システムであって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、第 1 解読制限を更新して得られる第 2 解読制限に基づいて前記コンテンツ鍵を生成する第 1 コンテンツ鍵生成手段と、前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第 1 暗号化手段とを具備し、前記復号化装置は、前記第 2 解読制限から前記コンテンツ鍵を生成する第 2 コンテンツ鍵生成手段と、前記暗号化コンテンツを前記第 2 コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第 1 復号化手段とを具備することを特徴とし、そのことにより上記目的が達成される。

【 0 0 1 4 】

前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて前記第 2 解読制限に更新する解読制限更新手段と、前記第 2 解読制限を時変鍵に基づいて暗号化し、第 1 暗号化解読制限を出力する第 2 暗号化手段とを具備し、前記暗号化

装置は、前記第 2 暗号化手段から転送される前記第 1 暗号化解読制限を前記時変鍵に基づいて復号化し、前記第 2 解読制限を生成する第 2 復号化手段とを具備し、前記第 1 コンテンツ鍵生成手段は、前記第 2 復号化手段により生成された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成してもよい。

## 【 0 0 1 5 】

前記暗号化装置は、共通鍵を記憶する第 1 共通鍵記憶手段と、前記第 1 解読制限を記憶する解読制限記憶手段と、第 1 乱数を生成する第 1 乱数発生手段と、前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化装置と相互認証処理を行なう第 1 相互認証処理手段と、前記第 1 相互認証処理手段における認証受理をうけて前記第 1 乱数と前記第 2 乱数とから前記時変鍵を生成する第 1 時変鍵生成手段と、前記第 1 解読制限を前記時変鍵を用いて暗号化して第 2 暗号化解読制限を出力する第 3 暗号化手段とをさらに具備し、前記復号化装置は、前記共通鍵を記憶する第 2 共通鍵記憶手段と、前記第 2 乱数を生成する第 2 乱数発生手段と、前記第 2 乱数と前記第 1 乱数とを用いて前記暗号化装置と相互認証を行なう第 2 相互認証処理手段と、前記第 2 相互認証処理手段における認証受理をうけて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する第 2 時変鍵生成手段と、前記第 2 暗号化解読制限を前記時変鍵を用いて復号化する第 3 復号化手段とを備えてもよい。

## 【 0 0 1 6 】

前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて第 2 解読制限に更新する第 1 解読制限更新手段をさらに備え、前記第 2 コンテンツ鍵生成手段は、前記第 1 解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成し、前記暗号化装置は、前記復号化装置の第 1 解読制限更新手段における解読制限の更新をうけて、前記第 1 解読制限を解読制限更新則に従って前記第 2 解読制限に更新する第 2 解読制限更新手段をさらに備え、前記第 1 コンテンツ鍵生成手段は、前記第 2 解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成してもよい。

## 【 0 0 1 7 】

前記暗号化装置は、前記共通鍵を記憶する第 1 共通鍵記憶手段と、前記第 1 解

読制限を記憶する読制限記憶手段と、第 1 乱数を生成する第 1 乱数発生手段と、前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化装置と相互認証を行なう第 1 相互認証処理手段と、前記第 1 相互認証処理手段における認証受理をうけて前記第 1 乱数と前記第 2 乱数とから時変鍵を生成する第 1 時変鍵生成手段と、前記第 1 読制限を前記時変鍵を用いて暗号化して暗号化読制限を出力する第 2 暗号化手段とを具備し、前記復号化装置は、前記共通鍵を記憶する第 2 共通鍵記憶手段と、前記第 2 乱数を生成する第 2 乱数発生手段と、前記第 2 乱数と前記第 1 乱数とを用いて前記暗号化装置と相互認証を行なう第 2 相互認証処理手段と、前記第 2 相互認証処理手段における認証受理をうけて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する第 2 時変鍵生成手段と、前記暗号化読制限を前記時変鍵を用いて復号化する第 2 復号化手段とを具備し、そのことにより上記目的が達成される。

## 【 0 0 1 8 】

前記第 2 読制限更新手段は、予め前記第 1 読制限を第 2 読制限に更新し、前記第 2 読制限更新手段は、前記第 1 コンテンツ鍵生成手段に更新された前記第 2 読制限を出力し、前記第 1 コンテンツ鍵生成手段は、前記第 2 読制限から前記コンテンツ鍵を生成し、前記第 2 読制限更新手段は、前記第 1 暗号化手段の処理が開始されたことをうけて、前記読制限記憶手段に前記第 2 読制限を格納してもよい。

## 【 0 0 1 9 】

前記第 1 および第 2 時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

## 【 0 0 2 0 】

前記第 1 および第 2 コンテンツ鍵生成手段は、前記第 2 読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

## 【 0 0 2 1 】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、前記第 1 および第 2 時変鍵生成手段は



、前記第 1 および第 2 乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【0022】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、前記第 1 および第 2 時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【0023】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、前記第 1 および第 2 コンテンツ鍵生成手段は、前記第 2 解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【0024】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第 1 および第 2 データ系列鍵生成手段をそれぞれさらに具備し、前記第 1 および第 2 コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【0025】

前記第 1 および第 2 相互認証処理手段は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証してもよい。

【0026】

本発明に係る暗号化装置は、コンテンツ鍵を用いて復号化装置と暗号通信を行う暗号化装置であって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、第 1 解読制限を更新して得られる第 2 解読制限に基づいて前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、前記コンテンツを前記コンテンツ鍵

に基づいて暗号化し、暗号化コンテンツを出力する第 1 暗号化手段とを具備し、そのことにより上記目的が達成される。

## 【 0 0 2 7 】

前記暗号化装置は、前記復号化装置から転送される第 1 暗号化解読制限を時変鍵に基づいて復号化し、前記第 2 解読制限を生成する復号化手段を具備し、前記コンテンツ鍵生成手段は、前記復号化手段により生成された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成してもよい。

## 【 0 0 2 8 】

前記暗号化装置は、共通鍵を記憶する共通鍵記憶手段と、前記第 1 解読制限を記憶する解読制限記憶手段と、第 1 乱数を生成する第 1 乱数発生手段と、前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化装置と相互認証処理を行なう相互認証処理手段と、前記相互認証処理手段における認証受理を受けて前記第 1 乱数と前記第 2 乱数とから前記時変鍵を生成する時変鍵生成手段と、前記第 1 解読制限を前記時変鍵を用いて暗号化して第 2 暗号化解読制限を出力する第 2 暗号化手段とをさらに具備してもよい。

## 【 0 0 2 9 】

前記暗号化装置は、前記復号化装置の解読制限の更新を受けて、前記第 1 解読制限を解読制限更新則に従って前記第 2 解読制限に更新する解読制限更新手段をさらに備え、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成してもよい。

## 【 0 0 3 0 】

前記暗号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、前記第 1 解読制限を記憶する解読制限記憶手段と、第 1 乱数を生成する第 1 乱数発生手段と、前記第 1 乱数と前記復号化装置から転送される第 2 乱数とを用いて前記復号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理を受けて前記第 1 乱数と前記第 2 乱数とから時変鍵を生成する時変鍵生成手段と、前記第 1 解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第 2 暗号化手段とを具備してもよい。

## 【 0 0 3 1 】

前記解読制限更新手段は、予め前記第 1 解読制限を第 2 解読制限に更新し、前記解読制限更新手段は、前記コンテンツ鍵生成手段に更新された前記第 2 解読制限を出力し、前記コンテンツ鍵生成手段は、前記第 2 解読制限から前記コンテンツ鍵を生成し、前記解読制限更新手段は、前記第 1 暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第 2 解読制限を格納してもよい。

## 【 0 0 3 2 】

前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

## 【 0 0 3 3 】

前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

## 【 0 0 3 4 】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

## 【 0 0 3 5 】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

## 【 0 0 3 6 】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

## 【 0 0 3 7 】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段

は、前記第 2 解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【 0 0 3 8 】

本発明に係る復号化装置は、コンテンツ鍵を用いて暗号化装置と暗号通信を行う復号化装置であって、前記復号化装置は、第 2 解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第 1 復号化手段とを具備し、そのことにより上記目的が達成される。

【 0 0 3 9 】

前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて前記第 2 解読制限に更新する解読制限更新手段と、前記第 2 解読制限を時変鍵に基づいて暗号化し、第 1 暗号化解読制限を出力する暗号化手段とを具備してもよい。

【 0 0 4 0 】

前記復号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、前記第 2 乱数を生成する乱数発生手段と、前記第 2 乱数と第 1 乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理を受けて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する時変鍵生成手段と、第 1 暗号化解読制限を前記時変鍵を用いて復号化する第 2 復号化手段とを備えてもよい。

【 0 0 4 1 】

前記復号化装置は、前記第 1 解読制限を解読制限更新則に基づいて第 2 解読制限に更新する解読制限更新手段をさらに備え、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第 2 解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【 0 0 4 2 】

前記復号化装置は、前記共通鍵を記憶する第 2 共通鍵記憶手段と、前記第 2 乱数を生成する第 2 乱数発生手段と、前記第 2 乱数と第 1 乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理を受けて前記第 2 乱数と前記第 1 乱数とから前記時変鍵を生成する時変

鍵生成手段と、暗号化解読制限を前記時変鍵を用いて復号化する第 2 復号化手段とを具備してもよい。

【 0 0 4 3 】

前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【 0 0 4 4 】

前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

【 0 0 4 5 】

前記前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【 0 0 4 6 】

前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第 1 および第 2 乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【 0 0 4 7 】

前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【 0 0 4 8 】

前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第 2 解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【 0 0 4 9 】

本発明では、デジタルコンテンツの暗号通信に用いる共通鍵の生成に解読制限を用いる。

【0050】

【発明の実施の形態】

以下に本発明の原理と実施の形態を添付の図面を用いて説明する。

【0051】

(実施の形態1)

図1は、本発明の実施の形態1における構成図を示し暗号化装置101と復号化装置102が暗号通信を行なうシステム100を示す。

【0052】

暗号化装置101は、共通鍵UKを記憶する共通鍵記憶部103と、解読制限を記憶する解読制限記憶部111と、コンテンツCTを記憶するコンテンツ記憶部121と、乱数R1を生成する乱数発生部105と、乱数R1と復号化装置102から転送される乱数R2と共通鍵UKとを用いて復号化装置102と相互認証処理を行なう相互認証処理部107と、相互認証処理部107における相互認証処理に応答して乱数R1と乱数R2とから相互認証処理が実行される度に可変な時変鍵VKを生成する時変鍵生成部109と、解読制限S1を時変鍵VKを用いて暗号化して暗号化解読制限S2を出力する暗号化部113と、復号化装置102の暗号化部116から転送される暗号化解読制限S3を時変鍵VKを用い解読制限S4に復号化し、解読制限記憶部111に書き込む復号化部115と、解読制限S4からコンテンツ鍵CKを生成するコンテンツ鍵生成部117と、コンテンツCTをコンテンツ鍵CKに基づいて暗号化し、暗号化コンテンツS5を出力する暗号化部119とを備える。

【0053】

復号化装置102は、共通鍵UKを記憶する共通鍵記憶部104と、乱数R2を生成する乱数発生部106と、乱数R2と乱数R1と共通鍵UKを用いて暗号化装置101と相互認証処理を行なう相互認証処理部108と、相互認証処理部108における相互認証処理に応答して乱数R2と乱数R1とから時変鍵VKを生成する時変鍵生成部110と、暗号化解読制限S2を時変鍵VKを用いて復号

化する復号化部 1 1 4 と、復号化部 1 1 4 で復号化した解読制限 S 1 を解読制限更新則に基づいて解読制限 S 4 に更新する解読制限更新部 1 1 2 と、解読制限 S 4 を時変鍵 V K を用いて暗号化し、暗号化解読制限 S 3 を出力する暗号化部 1 1 6 と、解読制限 S 4 からコンテンツ鍵 C K を生成するコンテンツ鍵生成部 1 1 8 と、暗号化コンテンツ S 5 をコンテンツ鍵 C K を用いて復号化し、コンテンツ C T を出力する復号化部 1 2 0 とを備える。

## 【 0 0 5 4 】

暗号化装置 1 0 1、復号化装置 1 0 2 はともに共通鍵記憶部 1 0 3、1 0 4 を備え同一の共通化鍵 U K を保持する。尚、予め共通化鍵 U K は同一共通鍵として共通鍵記憶部 1 0 3、1 0 4 に記憶されていてもよいし、作成プロセスにより同一の共通化鍵 U K を作成してもよい。

## 【 0 0 5 5 】

暗号化装置 1 0 1 は、解読制限 S 1 を記憶する解読制限記憶部 1 1 1 とコンテンツ C T を記憶するコンテンツ記憶部 1 2 1 を備える。なお、これら共通鍵記憶部 1 0 3、解読制限記憶部 1 1 1、コンテンツ記憶部 1 2 1 は外部から直接アクセスすることができないプロテクト領域に配置されている。

## 【 0 0 5 6 】

以下図 1 および図 2 を参照して、暗号化装置 1 0 1 と復号化装置 1 0 2 とを含むシステム 1 0 0 の処理手順を説明する。

## 【 0 0 5 7 】

暗号化装置 1 0 1、復号化装置 1 0 2 は、互いに独立に乱数 R 1、R 2 を発生する乱数発生部 1 0 5、1 0 6 を備え、互いの乱数 R 1、R 2 を交換し、乱数 R 1 と共通化鍵 U K を用いて応答値 V 1 を作成し、乱数 R 2 と共通化鍵 U K を用いて応答値 V 2 を作成し、応答値 V 1、V 2 を交換し、比較することによって相互に相手機器が正当な機器であることを認証するチャレンジレスポンス型の相互認証を相互認証処理部 1 0 7、1 0 8 で行なう (S 2 0 1)。

## 【 0 0 5 8 】

相互認証処理部 1 0 7、1 0 8 によって相手機器が正当であることを確認する認証確立が成立したか否かが判断される (S 2 0 2)。認証確立が成立しないと

判断された場合には（S 2 0 2 で N O）、処理は終了する。認証確立が成立したと判断された場合には（S 2 0 2 で Y E S）、時変鍵生成部 1 0 9、1 1 0 は互いの乱数 R 1、R 2 から相互認証毎に変化する同一の時変鍵 V K を生成する（S 2 0 3）。その後、暗号化装置 1 0 1 内の解読制限記憶部 1 1 1 に格納されている解読制限 S 1 を時変鍵 V K を用いて暗号化部 1 1 3 で暗号化して暗号化解読制限 S 2 を復号化装置 1 0 2 に転送する（S 2 0 4）。

## 【 0 0 5 9 】

復号化部 1 1 4 は受信した暗号化解読制限 S 2 を同じく時変鍵 V K を用いて復号化する（S 2 0 5）。復号化部 1 1 4 にて復号化された解読制限 S 1 を解読制限更新部 1 1 2 は解読制限更新則に従って更新し（S 2 0 6）、更新された解読制限 S 4 を時変鍵 V K を用いて暗号化して（S 2 0 7）暗号化解読制限 S 3 を暗号化装置 1 0 1 に転送する。復号化部 1 1 5 は、転送された暗号化解読制限 S 3 を時変鍵 V K を用いて復号化して更新された解読制限 S 4 を得て、解読制限記憶部 1 1 1 に格納する（S 2 0 8）。

## 【 0 0 6 0 】

コンテンツ鍵生成部 1 1 7 は解読制限 S 4 からコンテンツ鍵 C K を生成する（S 2 0 9）。コンテンツ記憶部 1 2 1 に格納されているコンテンツ C T を暗号化装置 1 0 1 から復号化装置 1 0 2 に転送する場合、暗号化部 1 1 9 はコンテンツ鍵 C K を用いてコンテンツ C T を暗号化する（S 2 1 0）。コンテンツ鍵生成部 1 1 8 は解読制限 S 4 からコンテンツ鍵 C K を生成する（S 2 1 1）。復号化装置内復号化部 1 2 0 はコンテンツ鍵 C K を用いて暗号化コンテンツ S 5 を復号する（S 2 1 2）。

## 【 0 0 6 1 】

なお、本実施の形態では、1 回の認証確立後コンテンツを暗号化装置から復号化装置に転送する例を示したが、認証確立後、送復号化装置間でコンテンツ転送が発生する毎に相手機器が正当であることを確認する相互認証を行うようにしてもよい。また、時変鍵 V K の生成に、相互認証に用いた乱数 R 1、R 2 を用いたが、応答値 V 1、V 2 を用いてもかまわない。

## 【 0 0 6 2 】



また、解読制限、コンテンツの暗号化および復号化に用いる方法は異なるアルゴリズムでも同一のアルゴリズムのものをを用いてよく、例えばDES (Data Encryption Standard) などを用いればよい。

【0063】

また、時変鍵、コンテンツ鍵の生成に用いる方法は異なるアルゴリズムでも同一のアルゴリズムのものをを用いてよく、例えばSHA (Secure Hash Algorithm) などの一方向性の関数を用いればよい。

【0064】

なお本実施の形態では本発明を分かりやすく説明するために、送受信を相互認証処理部107、108、暗号化部113、復号化部114、復号化部115、暗号化部116、暗号化部119、復号化部120が行っている例を示しているが、実際の送受信は、制御部122、123で管理されることが一般的である。後述する実施の形態でも同様である。

【0065】

以上のように、本実施の形態の著作物保護システムは、著作物であるコンテンツCTの転送において、解読制限の更新情報(解読制限S4)を関連させてコンテンツの暗号通信を行うので、正しく解読制限S1の更新処理を行わないと、コンテンツCTを解読できないという効果がある。

【0066】

(実施の形態2)

図2は、本発明の実施の形態2における著作物保護システム200を示す。図2において図1と同一の構成要素には同一の参照符号を付し、説明を省略する。

【0067】

著作物保護システム200では、図1で示した著作物保護システム100のように解読制限更新部112で更新された解読制限S4を暗号化／復号化を行なって転送し、解読制限記憶部111に格納するのではなく、暗号化装置201内にも解読制限更新部223を備える。

【0068】

復号化装置202の解読制限更新部212は、解読制限S1の更新を命令する

解読制限更新指令ＣＣだけを解読制限更新部２２３に転送する。解読制限更新部２２３は転送される解読制限更新指令ＣＣを受けとり、解読制限Ｓ１を更新し、更新した解読制限Ｓ４を解読制限記憶部２１１に格納する。

## 【００６９】

以上のように、本実施の形態の著作物保護システム２００は、コンテンツ鍵ＣＫの生成に関連する更新された解読制限Ｓ４を復号化装置２０２から暗号化装置２０１へ転送する必要がないため、解読制限Ｓ４の秘匿性を高めることができる。また、更新された解読制限Ｓ４の転送に係わる暗号化部、復号化部を削除することができるためシステム規模を小さくできるという効果がある。

## 【００７０】

## （実施の形態３）

図３は、本発明の実施の形態３における著作物保護システム３００を示す。図３において図１と同一の構成には同一の符号を付し説明を省略する。

## 【００７１】

著作物保護システム３００では、図２で示した著作物保護システム２００のように解読制限更新部２１２からの更新指令ＣＣをうけて暗号化装置２０１内の解読制限更新部２２３によって解読制限Ｓ１を更新するのではなく、予め暗号化装置３０１内の解読制限記憶部３１１に格納されている解読制限Ｓ１を解読制限更新部３２３によって更新する。コンテンツ鍵生成部１１７が更新された解読制限Ｓ４を用いてコンテンツ鍵ＣＫを生成し、暗号化部３１９がコンテンツＣＴの暗号化を開始することに応答して、解読制限更新部３２３は解読制限記憶部３１１に更新された解読制限Ｓ４を格納する。

## 【００７２】

以上のように、本実施の形態の著作物保護システム３００は、復号化装置３０２からの指令で解読制限Ｓ１を更新するのではなく、予め解読制限更新部３２３が解読制限Ｓ１を更新し、かつコンテンツ鍵生成部１１７がデータ転送鍵ＣＫを生成するので、処理ステップを短縮できるという効果がある。

## 【００７３】

## （実施の形態４）

図 4 は、本発明の実施の形態 4 における著作権保護システム 4 0 0 を示す。図 4 において図 1 と同一の構成には同一の符号を付し説明を省略する。

【 0 0 7 4 】

著作権保護システム 4 0 0 では、時変鍵生成部 4 0 9、4 1 0 における時変鍵 V K の生成において、乱数 R 1、R 2 に加えて共通鍵 U K を用いる。なお、時変鍵 V K は、例えば、乱数 R 1、R 2、共通鍵 U K を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。

【 0 0 7 5 】

以上のように、本実施の形態の著作権保護システム 4 0 0 によれば、外部でモニタ可能な乱数 R 1、R 2 だけから時変鍵 V K を生成するのではなく、秘密な共通鍵 U K を関連付けるようにして時変鍵 V K を生成しているので時変鍵 V K の類推が容易でなく、時変鍵 V K の秘匿性を向上させることができるという効果がある。

【 0 0 7 6 】

(実施の形態 5)

図 5 は、本発明の実施の形態 5 における著作権保護システム 5 0 0 を示す。図 5 において図 1 と同一の構成には同一の符号を付し説明を省略する。

【 0 0 7 7 】

著作権保護システム 5 0 0 では、コンテンツ鍵生成部 5 1 7、5 1 8 におけるコンテンツ鍵 C K の生成において、更新された解読制限 S 4 に加えて時変鍵 V K を用いる。なお、コンテンツ鍵 C K は、例えば、解読制限 S 4、時変鍵 V K を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。

【 0 0 7 8 】

以上のように、本実施の形態の著作権保護システム 5 0 0 によれば、更新された解読制限 S 4 だけから時変鍵 C K を生成するのではなく、相互認証毎に時系列的に変化する時変鍵 V K を関連付けるようにし、時変鍵 V K を生成しているので、よりコンテンツの暗号化の強度を向上させることができるという効果がある。

【 0 0 7 9 】

(実施の形態 6)

図 6 は、本発明の実施の形態 6 における著作権保護システム 6 0 0 を示す。図 6 において図 1 と同一の構成には同一の符号を付し説明を省略する。

#### 【 0 0 8 0 】

著作物保護システム 6 0 0 では、暗号化装置 6 0 1 および復号化装置 6 0 2 に入力または出力される入出力データの全体または一部（ここでは、乱数 R 1、R 2、応答値 V 1、V 2、暗号化解読制限 S 2、S 3、暗号化コンテンツ S 5）からデータ系列鍵 T K 1 を生成するデータ系列鍵生成部 6 2 5、6 2 6 を暗号化装置 6 0 1 および復号化装置 6 0 2 に備える。時変鍵生成部 6 0 9、6 1 0 およびコンテンツ鍵生成部 6 1 7、6 1 8 における鍵の生成にデータ系列鍵 T K 1 を加える。

#### 【 0 0 8 1 】

なお、データ系列鍵 T K 1 は、例えば、各入出力データの H i s t o r y をカウントして生成すればよい。また、時変鍵 V K は、例えば、乱数 R 1、R 2、データ系列鍵 T K 1 を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。また、コンテンツ鍵 C K は、解読制限 S 4、データ系列鍵 T K 1 を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。また、入出力される入出力データの全てからデータ系列鍵 T K 1 を生成する必要はなく、そのうちの一部から生成するようにしてもかまわない。

#### 【 0 0 8 2 】

以上のように、本実施の形態の著作権保護システム 6 0 0 は、送復号化装置毎に独立に入出力される入出力データを監視し、入出力データから各機器共通なデータ系列鍵 T K 1 を生成し、生成されたデータ系列鍵 T K 1 を各鍵の生成に関連付けるようにしている。暗号通信の対象となる送復号化装置間で入出力データが同一である必要があるため、通信のなりすましを防止することができるという効果がある。

#### 【 0 0 8 3 】

##### 【発明の効果】

以上のように本発明に係る著作物保護システムによれば、著作物であるコンテンツの転送において、解読制限の更新情報を関連させて暗号通信を行うので、正

しく解読制限の更新処理を行わないと、コンテンツを解読できない効果がある。

【 0 0 8 4 】

また、本発明に係る著作物保護システムは、データ転送鍵の生成に関連する更新された解読制限を転送しなくても良いため、秘匿性を高めることができる。また、更新された解読制限の転送に係わる暗号化部、復号化部を削除することができるためシステム規模を小さくできるという効果がある。

【 0 0 8 5 】

また、本発明に係る著作物保護システムは、復号化装置からの指令で解読制限を更新するのではなく、予め暗号化装置が解読制限を更新し、かつデータ転送鍵を生成しているので、処理ステップを短縮できるという効果がある。

【 0 0 8 6 】

また、本発明に係る著作物保護システムは、外部でモニタ可能な乱数だけから時変鍵を生成するのではなく、秘密な共通鍵を関連付けるようにしているので時変鍵の類推が容易でなく、秘匿性を向上させることができるという効果がある。

【図面の簡単な説明】

【図 1】

実施の形態 1 のシステムの構成を示す構成図である。

【図 2】

実施の形態 1 のシステムの処理手順を示すフローチャートである。

【図 3】

実施の形態 2 のシステムの構成を示す構成図である。

【図 4】

実施の形態 3 のシステムの構成を示す構成図である。

【図 5】

実施の形態 4 のシステムの構成を示す構成図である。

【図 6】

実施の形態 5 のシステムの構成を示す構成図である。

【図 7】

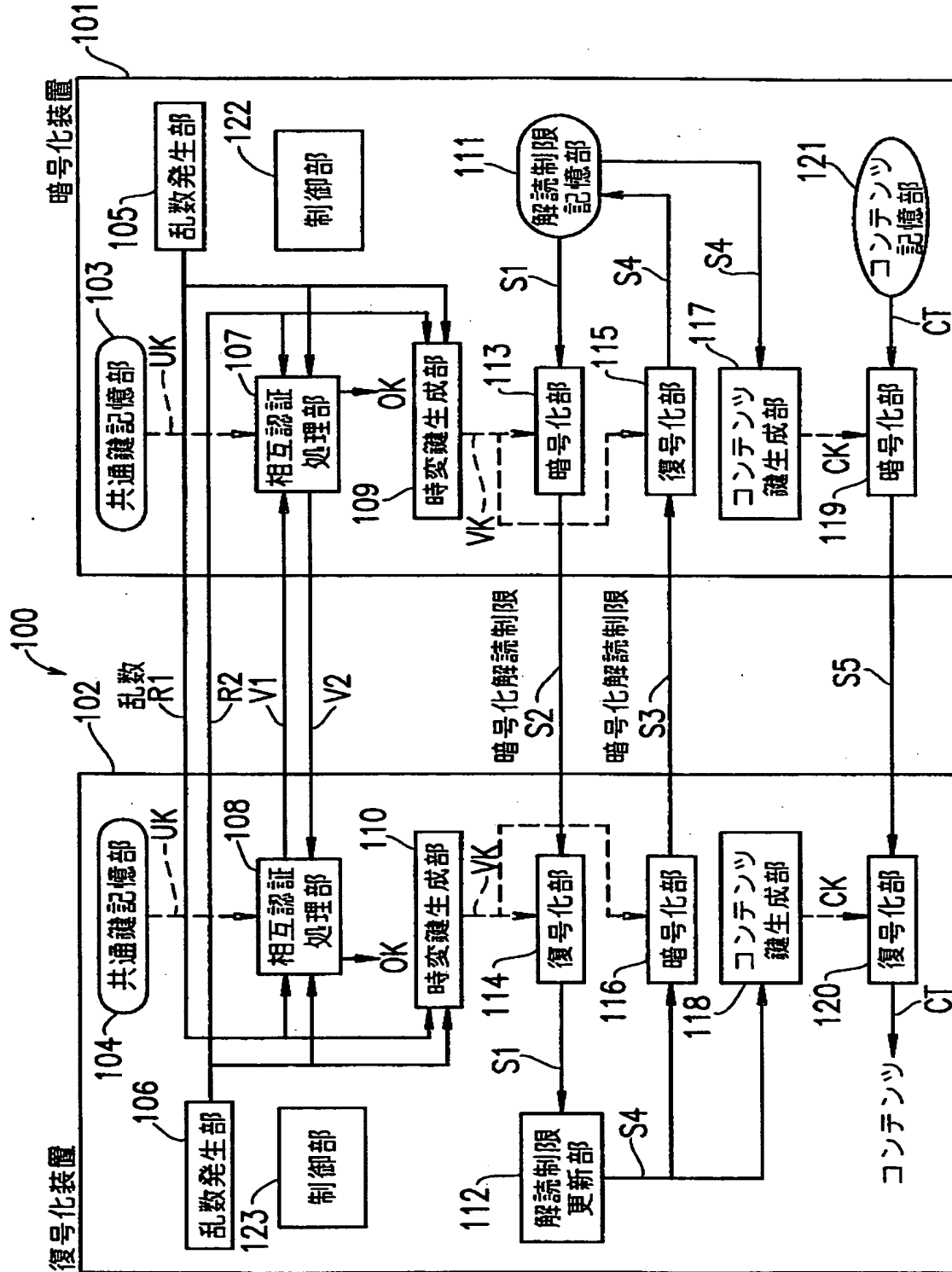
実施の形態 6 の構成を示す構成図である。

【符号の説明】

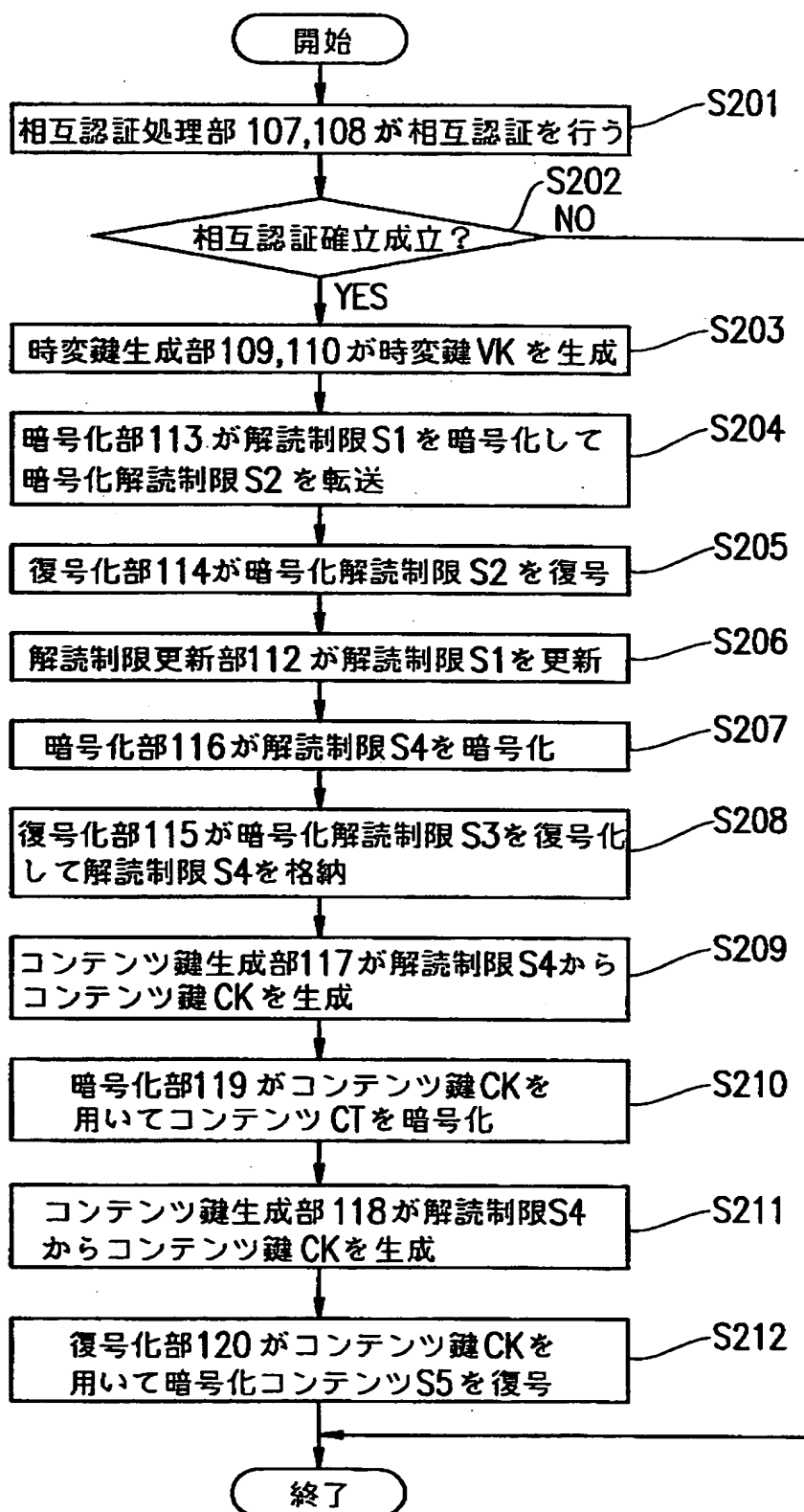
1 0 1、2 0 1、3 0 1、4 0 1、5 0 1、6 0 1	暗号化装置
1 0 2、2 0 2、3 0 2、4 0 2、5 0 2、6 0 2	復号化装置
1 0 3、1 0 4	共通鍵記憶部
1 0 5、1 0 6	乱数発生部
1 0 7、1 0 8	相互認証処理部
1 0 9、1 1 0、6 0 9、6 1 0	時変鍵生成部
1 1 1、2 1 1、3 1 1	解読制限記憶部
1 1 2、2 1 2、2 2 3、3 2 3	解読制限更新部
1 1 3、1 1 6、1 1 9	暗号化部
1 1 4、1 1 5、1 2 0	復号化部
1 1 7、1 1 8、6 1 7、6 1 8	コンテンツ鍵生成部
6 2 5、6 2 6	データ系列鍵生成部

【書類名】 図面

【図1】

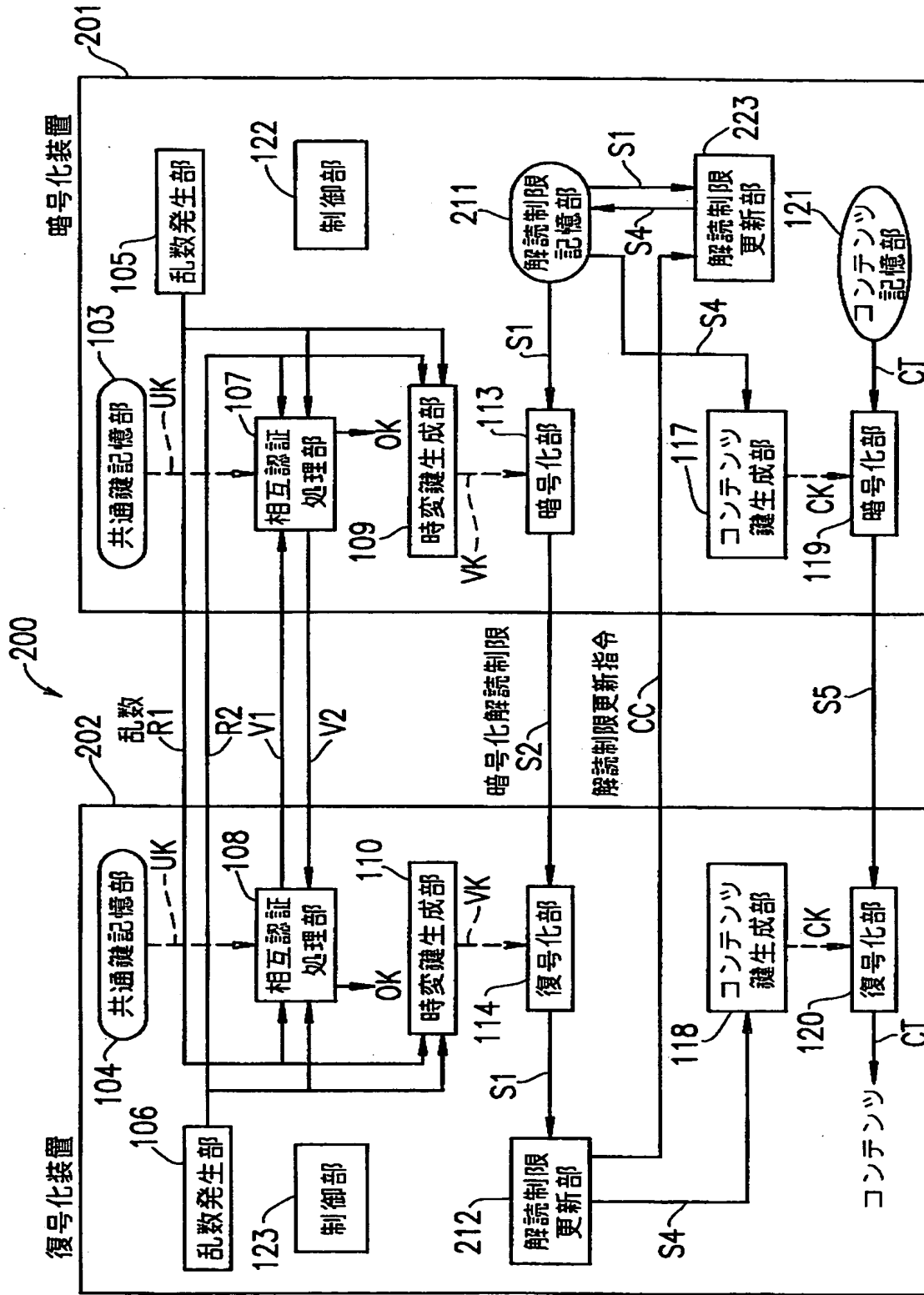


【図 2】

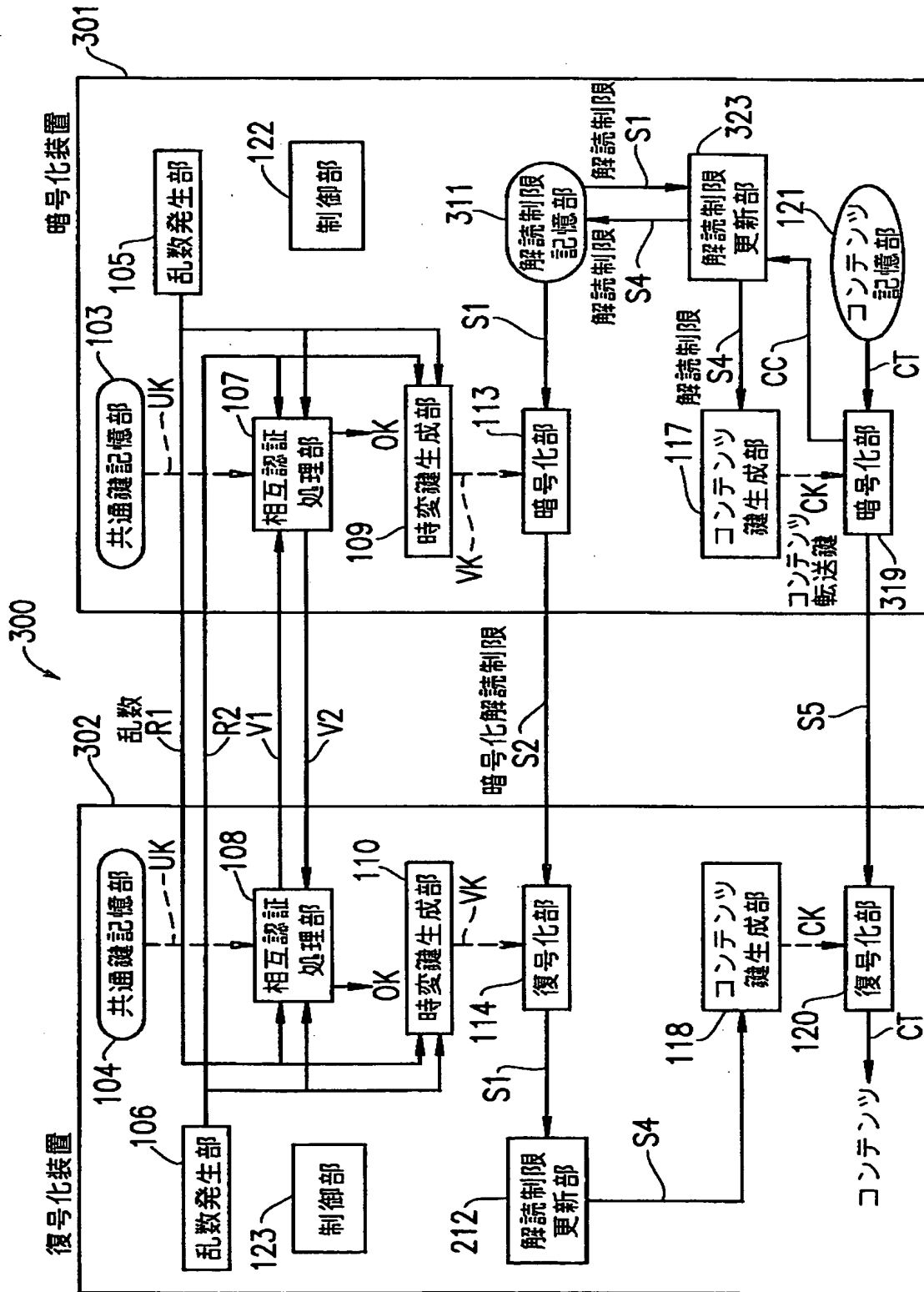




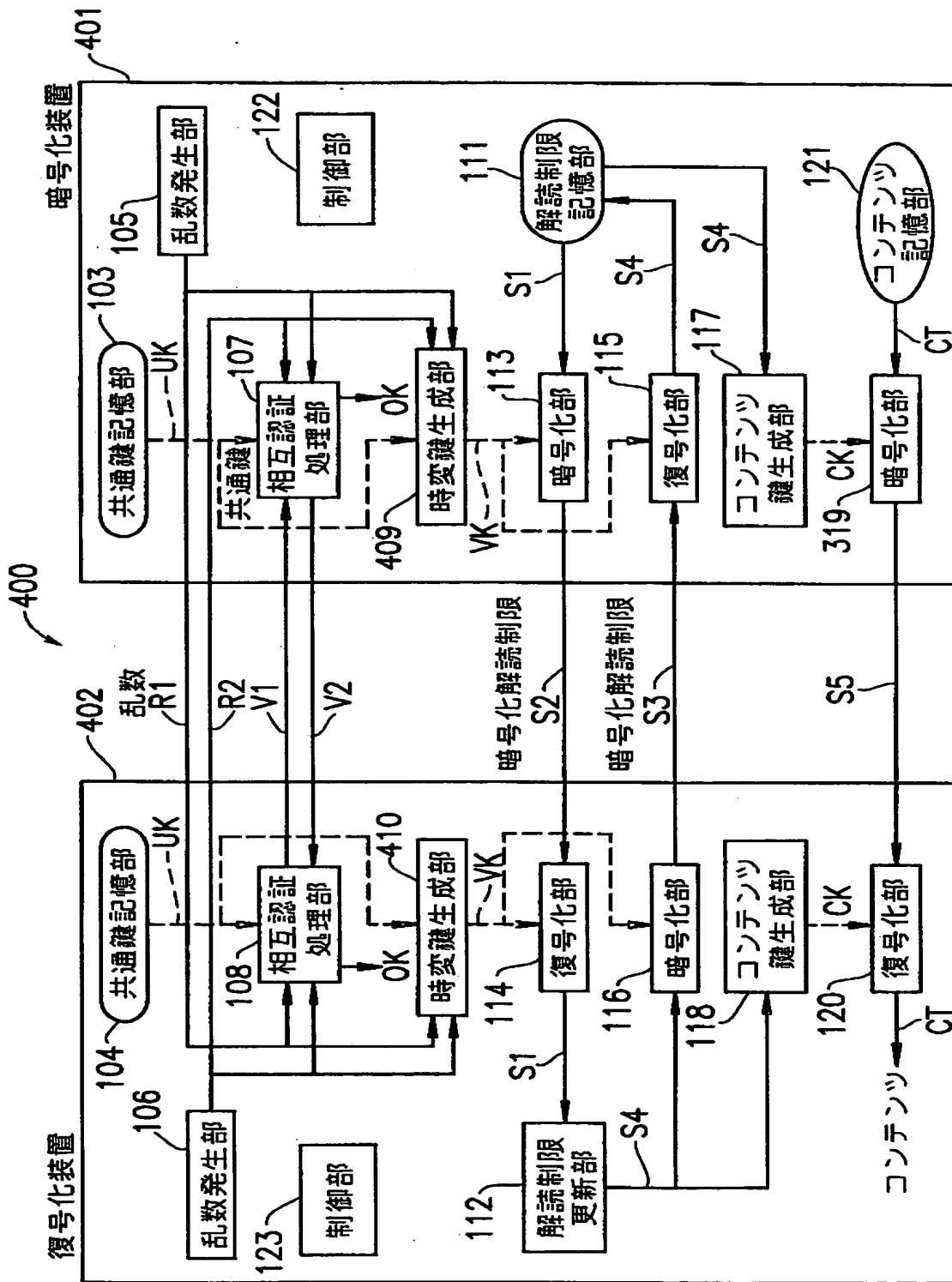
【図 3】



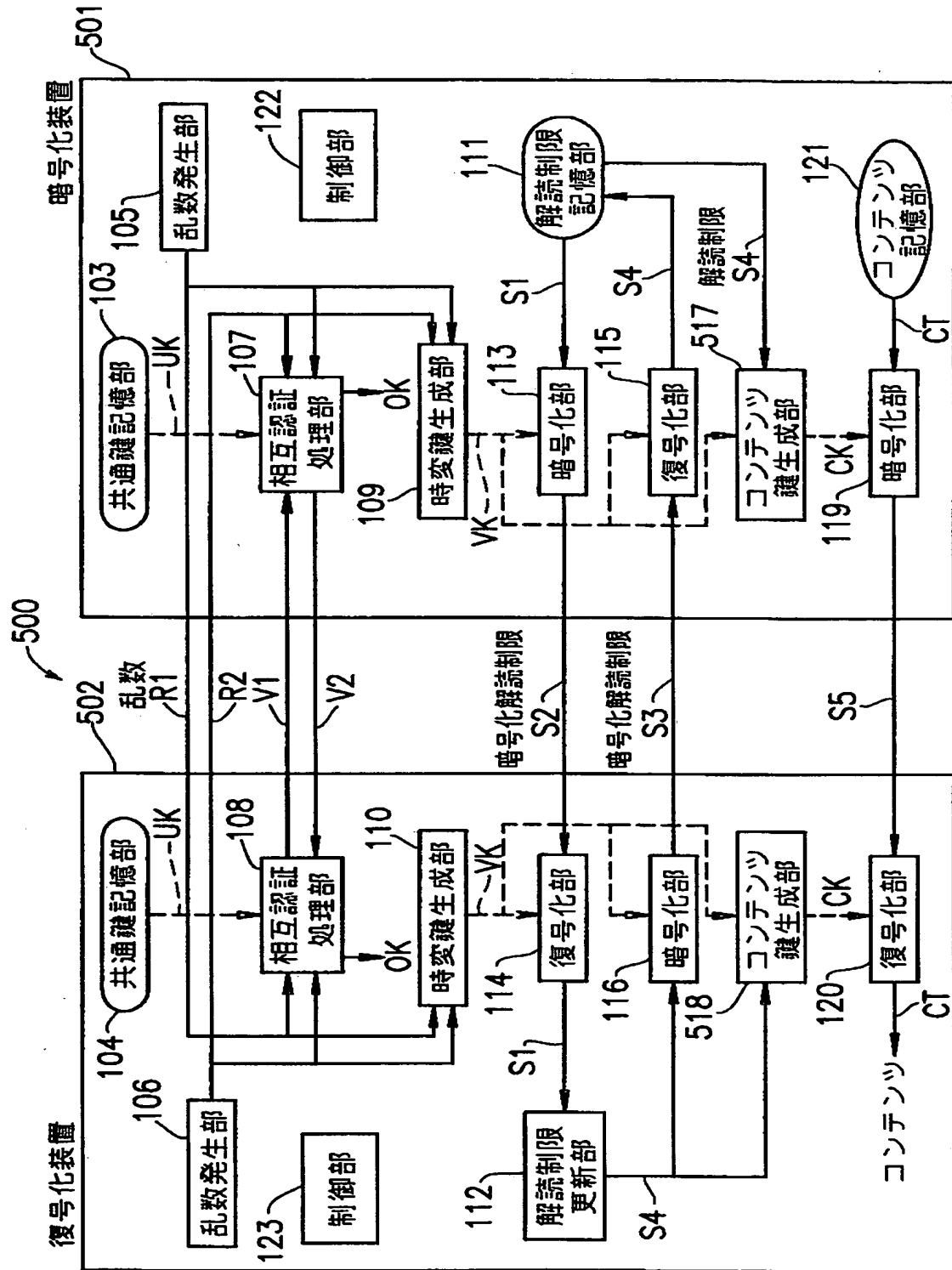
【図4】



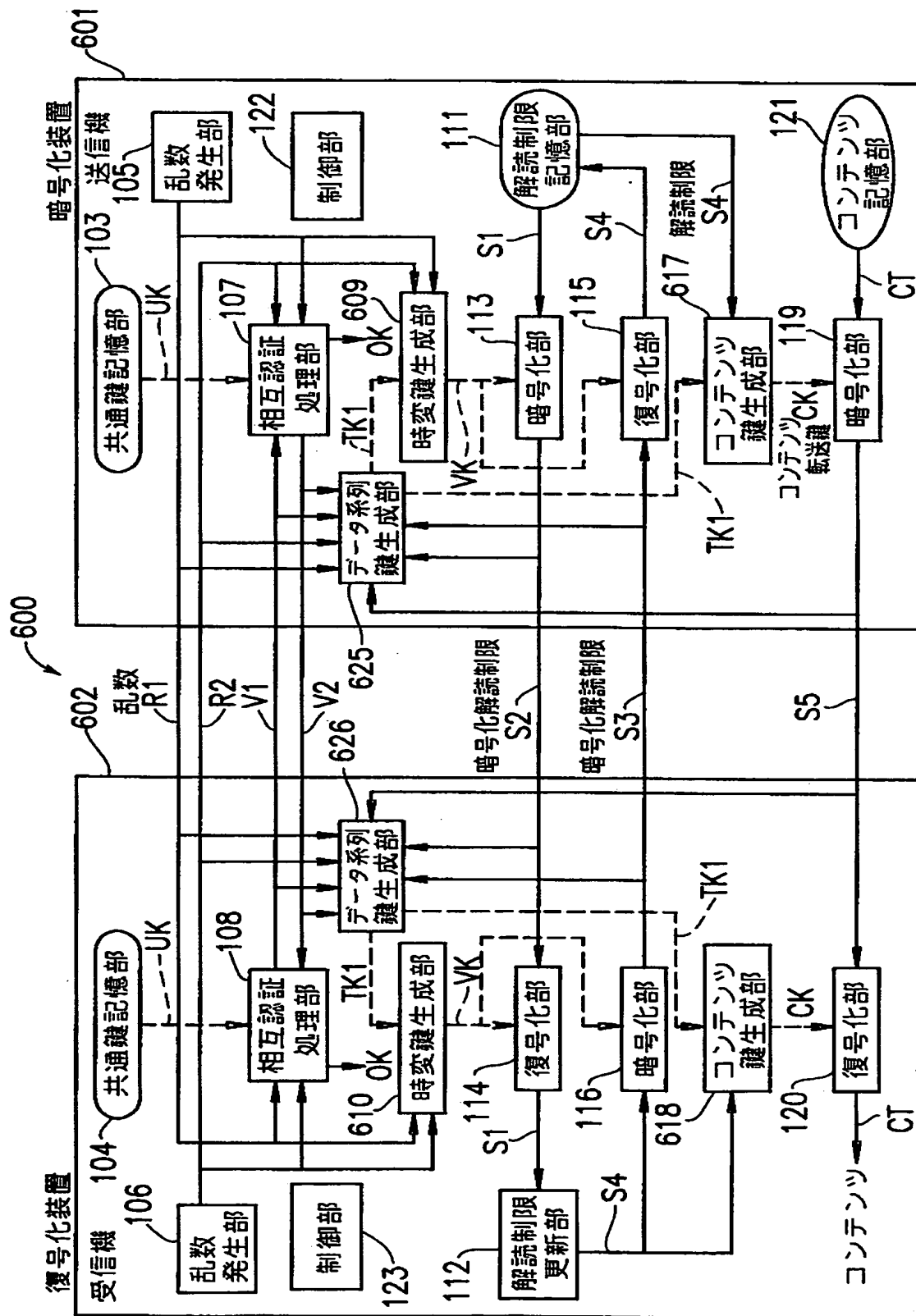
【図 5】



【図6】



【図 7】



【書類名】 要約書

【要約】

【課題】 記録媒体に記録された解読制限を持ったデジタルコンテンツの不正解読を防止するシステムを提供する。

【解決手段】 コンテンツ鍵の共有化とそのコンテンツ鍵を用いた暗号通信を行う暗号化装置および復号化装置から構成される通信システムにおいて、暗号化装置及び復号化装置は相互認証によって相手機器が正当な機器であることを認証し合い、かつ相互認証に用いた乱数から時変鍵を共有化する。復号化装置に格納されている再生回数データなどの解読制限を時変鍵で暗号化し、機密保護した状態で暗号化装置に転送し、かつ両機器において解読制限の更新を行い解読制限を共有化する。コンテンツのロードに際しては、更新された解読制限から生成したコンテンツ鍵を用いて暗号通信を行う構成とした。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社